

trusted alias maps that may, for example, identify multiple public key certificates to be associated with a single, or more than one, friendly email name.

The Chan reference is directed to a completely different system and operation. In particular, Chan teaches using a security identifier (SID) and access rights in the form of a bit mask wherein each bit may correspond to a permission. The security mechanism compares the security IDs in a token along with the type of action or actions requested by the process against entries in an access control list for example. If a match is found with an allowed user or group in the type of access desired, the process will be granted access otherwise access is denied. (See for example, paragraph 36). As such, there is no message header identifier described that is associated with a public key. The "Response to Arguments" section states that checking the SID is interpreted to constitute the determination of a digital signature verification error based on a received message header identifier associated with a public key certificate identifier. However, such an interpretation is inconsistent with the actual claim language and the actual teachings of the Chan reference. The office action does not indicate which "message" the Chan reference is referring to which contains a "message header identifier" that is associated with a "public key certificate identifier". The term "public key" does not appear to be mentioned in the Chan reference.

In addition, it appears that the only time Chan refers to email messages is with respect to the description of Fig. 16 and paragraphs 93-96 for example. However, even in this implementation, there is no generation of a digital signature verification map that contains a plurality of acceptable message header identifiers associated with the public key certificate identifier. The office action does not appear to address this limitation completely. For example, the office action cites to a different portion of the reference dealing with Internet websites and

not emails. In particular, the office action cites to the portion of the Chan reference (page 8 and 9) which describes, for example, that a restricted access may be implemented for uniform resource locator (URL) site identities. Again this cited portion does not deal with messages or message header identifiers or generating digital signature verification maps containing a plurality of acceptable message header identifiers wherein those plurality of acceptable message header identifiers are associated with public key certificate identifiers. If the rejection is maintained, Applicant respectfully requests the exact language being equated with the Applicant's claimed digital signature verification map as this term must be given meaning as defined in the claim.

For example, digital signature verification requires the verification of a digital signature and the map must contain a plurality of acceptable message header identifiers. In addition, the claim requires that these "plurality of acceptable message header identifiers" are associated with "a public key certificate identifier". The office action does not appear to address this claim language. Instead, the office action states "the office interprets that the combination of a unique URL and a binary certificate ID in an SID or another form constitutes a mapping..." However, Applicant is not claiming such a combination. The unique URL in Chan is not a message header nor is the binary certificate ID or SID as described in Chan a digital signature that is verified.

Also, the office action fails to identify in Chan which data is the plurality of acceptable message header identifiers that are associated with the public key certificate identifier as generated as a digital signature verification map. As such, since the unique URL is not a message header and since the SID is not a "message header identifier", and since these are not associated with a public key certificate, the cited portion does not render the claims unpatentable. Accordingly, the claims are in condition for allowance.

Moreover, the portion dealing with emails in the Chan reference again does not teach or suggest generating a digital signature verification map containing a plurality of acceptable message header identifiers associated with the public key certificate identifier since the SIDs that are described in the email embodiment appear merely to be prestored in a receiving unit and indicate restriction access based on an individual's email name. There is no digital signature verification error determined based on a received message header identifier and then generating a digital signature verification map that contains a plurality of acceptable message header identifiers that are associated with the public key certificate identifier as claimed. Accordingly, the claims are in condition for allowance.

As to claim 2, 5, 21, 24, 30 and 33, Applicant again reasserts the relevant remarks made in the previous office action. For example, as noted in Applicant's specification and Fig. 2, the digital signature verification map may include, for example, certificate subject identification information of multiple certificates that are associated with a single alias name. Such a digital signature verification map is not taught or suggested in the cited reference. Accordingly, these claims are also in condition for allowance.


As to the other dependent claims, Applicant reasserts the relevant remarks made in the previous office action. In addition, Applicant respectfully reasserts the relevant remarks made above since Chan also does not compare a public key certificate identifier with the message header identifier to determine if a mismatch is detected. The cited portion of the reference deals instead with software application and an API that operates to generate an error code. There does not appear to be any message header identifier employed in such an embodiment taught in Chan. Moreover, the words "digital signature" have meaning as known in the art which requires, for example, the use of a signing key to produce the digital signature. Such a scheme is not taught

or suggested in the cited portion of Chan. Accordingly, claims 9, 11, 13, 19, 20 and 37 are also in condition for allowance.

Accordingly, Applicant respectfully submits that the claims are in condition for allowance and that a timely Notice of Allowance be issued in this case. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

Date: 8/25/04

By: 
Christopher J. Reckamp
Registration No. 34,414

Vedder, Price, Kaufman & Kammholz, P. C.
222 N. LaSalle Street
Chicago, IL 60601
PHONE: (312) 609-7599
FAX: (312) 609-5005
E-MAIL: creckamp@vedderprice.com